# E-mails ondertekenen en versleutelen

# E-mails achter slot e

**Of je nu met zwier een aandoenlijke liefdesverklaring hebt neergepend, of heel sec je kredietkaartnummer hebt vermeld… zulke mailtjes hoeft niet iedereen te zien: ze zijn enkel bedoeld voor de ogen van de – juiste – ontvanger! Jammer genoeg steekt het e-mailmedium vol gaten en ogen en weet je nooit wie er allemaal tersluiks meekijkt. In dit dossier geven wij echter al die pottenkijkers het deksel op de neus…**

Zonnige groetjes uit Andalusië… veel meer dan zulke pasklare boodschappen wil je echt niet kwijt op een prentbriefkaart. Natuurlijk niet, want naast je eigen postbode zijn er nog tal van andere beambten die je kaart door de vingers krijgen! In een e-mailberichtje ben je echter best bereid heel wat meer vertrouwelijke nieuwtjes prijs te geven, maar is dat wel zo'n goed idee? Niet alleen blijft zo'n berichtje immers vaak achter op je eigen pc en moet je dus beducht zijn voor al te nieuwsgierige huisgenoten, dat geldt evenzeer voor de computer van de ontvanger. Maar op de weg tussen zender en ontvanger loert nog meer gevaar… Denk namelijk niet dat jouw berichtje rechtstreeks de pc van de ontvanger bereikt! Om te beginnen komt het mailtje eerst toe bij de *mailserver* van je provider en die is er bovendien wettelijk toe verplicht alle berichten enkele maanden te stockeren. Vandaar gaat het naar de volgende mailserver, en dat is nog niet noodzakelijk die van de ontvanger. Op elke tussenstop wordt het berichtje normaal enige tijd bijgehouden en kan het in principe door de operatoren van de server worden ingekeken. E-mailen verloopt vaak ook in alle haast, zodat je al snel een verkeerde ontvanger uit je adresboek hebt gepikt! En wie op meer James Bond-achtige scenario's is belust… de meeste mailservers mogen dan wel goed beveiligd zijn, soms slagen doortastende hackers er toch nog in zo'n machine te kraken. En dan zijn er ook nog *spoofers* die berichtjes versturen met vervalste afzendadressen – en misschien wel dat van jou (zie kaderstukje)? En wat te denken van 'legale' spionagepraktijken als Carnivore en Echelon, waarmee FBI en NSA het berichtenverkeer heimelijk monitoren op zoek naar verdachte communicatie…

## SPOOFEN VOOR BEGINNERS

Je hoeft echt geen doorgewinterde hacker te zijn om snel even een berichtje met een vervalst afzendadres te versturen! Wil je hier zelf mee stoeien, weet dan wel dat zoiets niet is toegelaten én dat deze vorm van spoofen bovendien niet waterdicht is: de sporen blijven onmiskenbaar in jouw richting wijzen. Wil je het toch uitproberen, stuur zo'n vervalst berichtje bij wijze van test dan enkel naar jezelf. Dat gaat ongeveer als volgt… Druk op de START-knop van Windows en selecteer UITVOEREN. Tik hier de opdracht COMMAND in en bevestig met OK. Je komt in een DOS-omgeving terecht. Hier tik je de volgende opdracht in: TELNET, gevolgd door de naam van de SMTP-server (uitgaande mail, kijk in je e-mailaccount) van je provider en de poort waarnaar die luistert (gewoonlijk is dat 25). In ons geval was dat bijvoorbeeld: TELNET SMTP.PANDORA.BE 25 (gevolgd door een druk op de ENTER-toets). Voor de rest kan je min of meer het verloop in de afbeelding volgen. Vermijd tikfouten, want zo'n telnetsessie registreert elk ingetikt teken en je backspace-toets haalt dan nog weinig uit.

```
Telnet
220 eos.telenet-ops.be ESMTP Postfix
helo George Bush
250 eos.telenet-ops.be
mail from: g.bush@whitehouse.gov
250 Ok
rcpt to: tvd@websight.be
250 Ok
data
354 End data with <CR><LF>.<CR><LF>
from: g.bush@whitehouse.gov
to: tvd@websight.be
subject: important meeting

Hi,
this is George - remember?
I want to meet you, but call me back first!
I don't trust e-mail, you see ! ;->

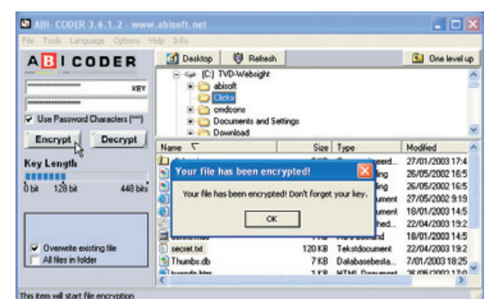
Bye!
.
250 Ok: queued as D36811FF7E
quit
221 Bye

De verbinding met de host is verbroken.

C:\>_
```

*Spoofen… makkelijk, maar niet wettelijk.*

## Dezelfde sleutel




*Nu nog het wachtwoord tot bij de ontvanger krijgen…*

Het zal al wel duidelijk zijn: e-mails zijn weinig meer dan digitale prentbriefkaarten! Om je toch van enige privacy te verzekeren, kan je natuurlijk aan het sleutelen gaan. En dat mag je vrij letterlijk nemen: je kan je boodschap versleutelen zodat hij voor een niet-ingewijde lezer onbegrijpelijk wordt. Een beetje zoals Caesar al deed toen die zijn boodschappers opzadelde met een geschreven tekst als "Ydo ddq!" en hen tegelijk de geheime sleutel in het oor fluisterde: "zeg aan de ontvanger dat hij telkens drie letters in het alfabet terug moet gaan". Natuurlijk hoef je die versleuteling niet manueel te doen: er zijn genoeg programma's waarmee je aan de hand van een wachtwoord

# n grendel!

CONTACTEER EENS EEN PRIVÉ DETECTIVE EMMA!
WAAROM MENEER ?
OM MIJN MAIL TE SCHADUWEN!!

een bestand (zoals een e-mailbijlage) kan encrypteren. Dat kan je bijvoorbeeld doen vanuit een toepassing als MS Word, of via het sharewarepakketje ABI-Coder [ www.abisoft.net/bd.html ], of met een gratis compressieprogramma als ZipGenius [ www.zipgenius.it/downloads_eng.asp ]. Zulke programma's maken gebruik van symmetrische encryptie, precies omdat ze met eenzelfde sleutel werken, zowel aan de kant van de zender (versleutelen, encrypteren of coderen) als aan de zijde van de ontvanger (ontsleutelen, decrypteren of decoderen). Het grote probleem is natuurlijk die sleutel – in dit geval: wachtwoord – bij je ontvanger te krijgen! Bovendien vergt het enige inspanning om je boodschap telkens in zo'n versleutelde bijlage te stoppen...

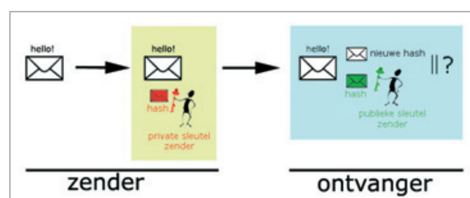
## Ieder voor zich

Knappe cryptologen hebben echter een systeem met twee sleutels uitgedokterd: de zogenaamde 'asymmetrische encryptie'. Je beschikt dan zowel over een private sleutel, die je absoluut geheim moet houden, als over een publieke sleutel die je aan iedereen ter beschikking mag stellen. Beide sleutels zijn weliswaar via een complexe wiskundige formule aan elkaar gelinkt, maar toch kan je de private sleutel niet afleiden uit z'n openbare tegenhanger – tenzij je er misschien enkele jaren een aantal supercomputers op loslaat. Ziet er best indrukwekkend uit, maar hoe werkt zo'n asymmetrisch encryptiesysteem nu eigenlijk?



*Je private sleutel kan je zelfs op een token opslaan.*

Stel, je tikt een vertrouwelijk e-mailtje in. Vooraleer je het verstuurt, bewerk je het eerst met je private sleutel die bijvoorbeeld veilig op je harde schijf is opgeslagen, of zich eventueel zelfs op een speciaal token of een smartcard zou kunnen bevinden. Heel concreet gebeurt er dan het volgende met je berichtje: er wordt een verkorte versie van gemaakt (een zogenaamde hash) en die wordt met je private sleutel geëncrypteerd. Deze versleutelde hash wordt vervolgens, samen met je publieke sleutel, automatisch mee met je bericht verstuurd.

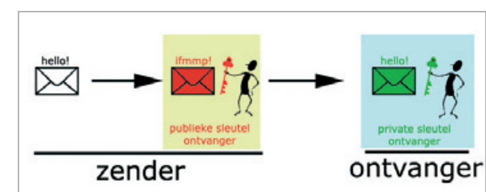



*Zo ziet ondertekende berichtgeving eruit.*

Zodra de ontvanger jouw berichtje binnenkrijgt, zal zijn e-mailprogramma opnieuw zo'n hash berekenen en ook jouw meegestuurde hash met behulp van je publieke sleutel decrypteren. Beide hashes worden vervolgens vergeleken en blijken die identiek te zijn, dan weet de ontvanger dat er onderweg niemand met het berichtje heeft geknoeid. In het andere geval trekt het e-mailprogramma van de ontvanger meteen aan de alarmbel! Bovendien weet hij dat jij inderdaad de afzender bent aangezien de hash met jouw publieke sleutel kon worden gedecrypteerd, en dat kan alleen maar als die met jouw private sleutel was geëncrypteerd. Herinner je: beide sleutels zijn namelijk mathematisch aan elkaar gelinkt! Op die manier weet de ontvanger zich al van drie zaken verzekerd: de **integriteit** van het berichtje – de minste wijziging onderweg zou tot verschillende hashes hebben geleid, de **authenticiteit** van de verzender – aangezien enkel jij over je private sleutel beschikt, én de **onweerlegbaarheid** van het berichtje – de verzender kan niet ontkennen het mailtje te hebben verstuurd.

## En de privacy?

Allemaal goed en wel, maar dat lost nog niet het probleem van de privacy of **confidentialiteit** op, en daar was het ons toch in de eerste plaats om te doen! Immers, het berichtje zelf is niet versleuteld en kan onderweg dus nog door derden worden gelezen. Gelukkig schiet ons ook op dit punt de asymmetrische encryptie ter hulp. Die laat ons namelijk tevens toe het hele berichtje, inclusief eventuele bijlagen, te versleutelen. Dat gaat ongeveer als volgt. Nadat je het berichtje ondertekend hebt, encrypteer je het geheel met de publieke sleutel van de ontvanger naar wie je het bericht wil versturen. Ook deze procedure verloopt heel transparant, en die publieke sleutel kan je altijd wel ergens te pakken krijgen: ofwel on line (zie verder), ofwel heb je van die persoon zelf al een ondertekend berichtje ontvangen en dan beschik je in principe meteen over z'n publieke sleutel. Komt je bericht toe bij de ontvanger, dan kan hij – en enkel hij! – het vervolgens weer ontsleutelen met zijn private sleutel. Het probleem van de confidentialiteit is hiermee eindelijk van de baan!




*Zo ziet gecodeerde berichtgeving eruit.*

## VAKTAAL

**Mailserver:** Een mailserver is een computer die de ontvangst en verzending van elektronische post verzorgt.

**Spoofen:** Spoofen is het vervalsen van het IP-adres van de afzender van een e-mail. Het wordt meestal gebruikt om de identiteit van die afzender te verbergen. Zo kan een netwerkbeheerder van de ontvangende host heel moeilijk de hacker identificeren.

## CREATIEF MET CERTIFICATEN

Digitale certificaten lenen zich dus wonderwel voor het versturen van beveiligde berichtjes. Maar daar eindigt het niet bij. Zo kan men bijvoorbeeld ook een webserver zodanig configureren dat enkel de surfers met een geldig certificaat toegang krijgen. Probeer maar even binnen te geraken op [ https://admin.globalsign.net/ra ]! Je kan certificaten trouwens ook inzetten om een versleutelde communicatie tussen webserver en browser op te zetten, zodat onverlaten vergeefs naar je doorgestuurde kredietkaartgegevens graaien. Zo'n surfsessie kan je herkennen aan een hangslot-pictogram onderaan je browser. En MyCertipost – een samenwerking tussen de Post en Belgacom, en zowat de opvolger van het Postbox-initiatief – zal heel binnenkort toelaten dat je via zo'n certificaat on line een aangetekend schrijven kan versturen. Inschrijven kan je alvast op [ www.mycertipost.be ].




*Halt! Certificaat aub!*




*Hmm... toch geen dubieus certificaat?*

## Valse sleutels

Zeer kritische lezers zitten nu wel met een prangende vraag... Hoe weet de ontvanger dat het sleutelpaar effectief bij de juiste verzender hoort? Stel, Piet heeft nog geen sleutelpaar. Een doortrapte spoofer verstuurt nu een berichtje naar een nietsvermoedende Pol met het afzendadres van Piet. Dit berichtje heeft de spoofer met z'n eigen private sleutel ondertekend en stuurt tegelijk z'n eigen publieke sleutel mee. Het berichtje komt aan bij Pol, en zijn e-mailprogramma weet hem niks beters te vertellen dan dat beide hashes kloppen en... het berichtje dus wel degelijk van (het e-mailadres van) Piet afkomstig is! Om zoiets te vermijden zou je eigenlijk bij een erkende instantie moeten kunnen aankloppen die zo'n sleutelpaar enkel toekent aan de persoon die inderdaad kan bewijzen dat hij is wie hij beweert te zijn, en die ook effectief over dat e-mailadres beschikt. Zo'n instantie valt enigszins te vergelijken met de officiële instanties (zoals gemeentebestuur of politiebureau) die ook eerst grondig je persoonsgegevens checken alvorens je een identiteitskaart of rijbewijs toe te kennen.




*On line zoeken naar digitale certificaten bij GlobalSign.*

Welnu, zulke instanties bestaan wel degelijk. In België kan je hiervoor onder meer aankloppen bij GlobalSign, dat intussen bij het bedrijf Ubizen hoort [ www.globalsign.net/digital_certificate/personalsign/index.cfm ]. Maar op het internet vind je ook nog andere diensten, zoals het bekende VeriSign [ www.verisign.com/products/class1 ] waar je in principe ook terechtkan. Wat moet je je nu precies voorstellen bij zulke diensten? Zij leveren zogenaamde digitale certificaten af. Zo'n certificaat behelst niet veel meer dan een digitale publieke sleutel die gekoppeld is aan de identiteit van de eigenaar. De private sleutel die hiermee samenhangt, wordt dan op de computer van de bezitter berekend.

Hoe stelt zo'n certificatie-autoriteit nu de identiteit van de aanvrager vast? Dat hangt een beetje af van welke klasse van digitaal certificaat je beoogt. Als we het bij een eenvoudig persoonlijk certificaat houden (zoals PersonalSign 2), dan kan bijvoorbeeld je e-mailadres en een fax met een kopie van je identiteitskaart volstaan (kostprijs bij GlobalSign voor 1 jaar: € 19,36 – voor elk volgend jaar: € 14,52). Ga je een trapje hoger (PersonalSign 3 Pro), dan moet je persoonlijk verschijnen voor een erkende registratie-autoriteit zoals de Kamer van Koophandel (€ 60,50 voor het eerste jaar – € 45,98 voor elk volgend jaar). Als de hele procedure achter de rug is, zal de certificatie-autoriteit normaal meteen ook je publieke sleutel bekend maken via on line lijsten op zijn site. In onze mini-workshop van dit artikel lees je hoe je een gratis demo-certificaat van GlobalSign kan afhalen, en hoe je er beveiligde mailtjes mee verstuurt. Kortom, gewapend met zo'n digitaal certificaat, kan weinig je nog weerhouden je liefdesverklaringen naar je bankdirecteur, en je kredietkaartnummer naar je geliefde te mailen – of was het nu omgekeerd?

## PGP: EIGEN KOERS?

PGP (Pretty Good Privacy) is een andere, erg populaire beveiligingsstandaard. Je kan PGP in de vorm van freeware downloaden op [ www.pgpi.org ]. In tegenstelling tot S/MIME (zie verder) gaat het in feite om een apart programma dat zich weliswaar net iets minder goed in je e-mailprogramma integreert, maar anderzijds kan PGP in principe overweg met elk e-mailprogramma (dus ook de niet-S/MIME compatibele). Nadeel dan weer is dat beide partijen PGP moeten geïnstalleerd hebben om een beveiligde communicatie te kunnen opzetten.




*Ook met PGP kan je berichten (en bestanden) signeren en coderen.*

# Doe het zelf!



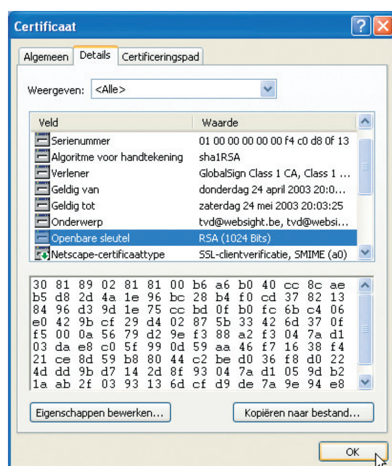

*Een demo-certificaat in acht stapjes.*

## Stap 1
### Je eigen certificaat

Wil je gedurende dertig dagen gratis een digitaal certificaat uitproberen, surf dan naar [ **www.globalsign.net/secure_demo.cfm** ]. Daar volg je de on line instructies op, die in duidelijke stappen zijn opgedeeld. Op een bepaald ogenblik krijg je dan een berichtje in je mailbox met een link. Die klik je vervolgens aan om de procedure verder te zetten. Even later krijg je nogmaals een mailtje waarmee je het certificaat kan downloaden en op je pc installeren. Deze hele procedure hoeft niet meer dan vijf minuten in beslag te nemen.

## Stap 2
### Hoe ziet het eruit?

Het geïnstalleerde certificaat kan je als volgt opvragen: open Internet Explorer, ga naar het menu Extra, selecteer Internet-opties, open het tabblad Inhoud en druk op de knop Certificaten. Selecteer je gloednieuwe certificaat en druk ten slotte op de knop Weergeven.




*Zo ziet een publieke sleutel (van een pas geïnstalleerd certificaat) eruit.*

## Stap 3
### Onderteken je mail

Open Outlook Express, en druk op de knop Nieuw bericht. Tik zoals gewoonlijk de gewenste velden in, en druk voor je het bericht verzendt op de knop Ondertekenen. Vind je die nergens terug in de knoppenbalk, dan kan je nog altijd terecht in het menu Extra.



| ! | 0 | Naar | Onderwerp |
|---|---|---|---|
| | | Toon Van Daele | Dit bericht heb ik ondertekend |
| | | Toon Van Daele | Dit bericht heb ik zowel ondertekend als gecodeerd |
| | | Toon Van Daele | Dit bericht heb ik gecodeerd |

*Ondertekende en/of gecodeerde berichtjes staan klaar in Postvak UIT.*

## Stap 4
### Encrypteren maar!

Een bericht encrypteren of coderen gaat ongeveer op dezelfde manier als in de voorgaande stap, alleen kies je hier de optie Coderen. In je Postvak UIT merk je intussen al dat deze berichtjes een speciaal pictogram hebben meegekregen...

## Stap 5
### Een ondertekend en gecodeerd bericht lezen

Krijg je een berichtje binnen dat ondertekend en/of gecodeerd werd, dan krijg je de inhoud normaal niet onmiddellijk te lezen, maar laat Outlook Express je eerst wat uitleg zien. Pas als je op de knop Doorgaan drukt, krijg je de eigenlijke boodschap te lezen – als tenminste alles in orde is met het certificaat en de verzending! Zet je echter een vinkje naast Dit Help-venster niet meer weergeven, dan krijg je dit helpvenster niet meer te zien, en verloopt de procedure zo goed als transparant, zowel voor zender als voor ontvanger. Voorwaarde evenwel is dat je van een e-mailprogramma gebruik maakt dat de zogenaamde S/MIME-standaard ondersteunt (Secure Multipurpose Mail Extensions). Het is niet nodig je daar veel zorgen om te maken, want zowel Outlook als Outlook Express (voor Windows) lopen mooi in de pas, en dat geldt ook voor Netscape Messenger (versies 4 en 7). Eudora is weliswaar iets koppiger, maar normaal kan je je ook daar uit de slag trekken met een




*Outlook Express stelt de ontvanger op z'n gemak...*

speciale plug-in. En voor wie zich afvraagt hoe een niet-compatibel e-mailprogramma zich gedraagt: ondertekende berichtjes komen dan als gewone berichtjes binnen, maar gecodeerde berichtjes... blijven jammer genoeg onleesbaar. Toch nog dit: mocht je certificaat ooit vervallen, dan is het misschien geen slecht idee het toch bij te houden! Je hebt het immers nodig wil je in je e-mailarchief ooit nog gecodeerde berichtjes – en bijlagen! – lezen, die met behulp van dat certificaat werden aangemaakt!

— Toon Van Daele —

## Een gratis digitaal certificaat voor 50 Clickx-lezers!

Globalsign heeft op het Clickx-kantoor 50 digitale certificaten (PersonalSign 2, geldigheid 1 jaar, waarde € 19,36) bezorgd. Die kunnen we verdelen onder onze lezers. Wil jij zo'n certificaat ontvangen? Surf dan nu naar onze website [ **www.clickxmagazine.be** ] en antwoord op de wedstrijdvraag! De winnaars worden persoonlijk verwittigd.